UNIVERSITY OF LEICESTER

Data Protection (GDPR) Guidance Note No. 21

Transferring personal data (GUIDANCE FOR ALL STAFF)

When data is sent from one point to another there is a risk of accidental loss or deliberate theft of data. Therefore, it is important that we all carefully consider if and how we should securely transfer data. This guidance outlines some of the key principles involved in transferring data securely.

Is it legal or acceptable to transfer data?

- Firstly, it is important to consider whether you are legally allowed to transfer personal data. Contracts or data sharing agreements governing the use of data might prohibit this. Also, if you are transferring personal data then this transfer should be documented in an appropriate privacy notice.
- What data should you be sending? Do you need to send everything or can you send a smaller quantity of data, potentially without including some of the more sensitive elements of personal data?
- Some contracts/data sharing agreements might prohibit sending data over the internet

What are the risks associated with sending personal data?

- Information is sent to the wrong recipient
- Information is intercepted during the data transfer
- Information is disclosed while in storage
- It is important to assess the risk likelihood and impact when considering a transfer method

What are some of the impacts of a data breach?

- Distress or embarrassment to an individual (or individuals)
- Damage to the University's reputation or operations
- Breach in legislation or contract with a possible financial penalty
- Risk to the wellbeing of an individual (or individuals)
- Substantial legal consequences
- Significant financial penalties

Types of Data

Public:	Publicly available information
Unrestricted:	Information that is not in the public domain but would cause minimal harm should unauthorised disclosure occur
Restricted:	Information which could cause harm or distress, to individuals or the University should unauthorised disclosure occur
Highly restricted:	Information which is likely to cause serious harm to individuals or the University should unauthorised disclosure occur

UNIVERSITY OF LEICESTER

Data Protection (GDPR) Guidance Note No. 21

What is the most appropriate transfer method?

Method	Description	Risks	Un-restricted	Restricted	Highly Restricted
OneDrive	➢ Office365 has been assessed by IT Services and is viewed as technically secure. ➢ Staff should be aware that human error (e.g. sharing documents with the wrong person) may be an issue so should careful check before sharing documents too widely.	➢ Data storage is linked to an individual's account and if they leave data will be deleted (where it might actually need to be retained for a set period) ➢ Can only be shared internally ➢ The permissions to access data are personally managed and can be vulnerable to user error ➢ Data can still be downloaded and kept locally risking duplication of data	✓	✓	✗
FileDrop	➢ FileDrop is a service that can securely transfer files from one individual to another. ➢ It is recommended that documents being transferred via FileDrop are encrypted (see below). ➢ Information is encrypted throughout the transfer. ➢ An email notification is sent when the transfer has been completed. ➢ Data is deleted from FileDrop after 30 days	➢ Data will be sent as a copy so there will be some degree of data duplication ➢ User must encrypt file first ➢ The process is still susceptible to user error when sending (which is why the file should be encrypted first)	✓	✓	✓
Sending via email:	➢ Email sent between two UoL email addresses is encrypted. ➢ Email sent to external email addresses (and vice versa) is generally encrypted (using opportunistic encryption), though this may not be the case for all points of the transfer. ➢ Extreme care should be taken over addressing an email	➢ Email is not always encrypted throughout the whole transfer ➢ Email can be intercepted ➢ You have no control over the data once it's left the organisation ➢ Duplication of data occurs by the existence of copies (in sent files etc.) ➢ Risk of misaddressing emails is high and	✓	✗	✗

Method	Description	Risks	Un-restricted	Restricted	Highly Restricted
	➢ It is recommended that 7:Zip encryption (see below) is used when emailing personal data ➢ It is advisable to be clear with the recipient of the data what they should do with it (i.e. not sending to other parties or storing local copies)	users often won't be aware they have misaddressed it unless informed ➢ No audit over whether the data has been received correctly ➢ High risk of emails being sent to a group email address rather than an individual			
Internal Mail:	➢ Consider what practical safeguards should be put in place as data will be handled by multiple parties ➢ If you need to transfer sensitive data you should personally take the information to the recipient	➢ Data is likely to be located in a public space during the process ➢ Data will physically be in numerous locations ➢ No audit of where the data has gone or been received ➢ Little chance of finding the data if it goes missing	✓	✗	✗
Encrypted hard drive/ external media	➢ The storage media itself will be protected ➢ When using this methods consider using a reliable and secure courier ➢ ITS can recommend certain memory sticks ➢ For large data sets end-user support in IT Services will provide recommendations on finding the correct type of hard drive. ➢ This method might be appropriate if you are contractually obliged not to send data over the internet	➢ Expensive ➢ Need to physically take the external media to the recipient ➢ Not always practical	✓	✓	✓
Fax:	➢ Not recommended for sending personal data ➢ There are risks associated with where the fax machined may be located at the recipient's end (i.e. they could be in a public location).	➢ Fax machine likely to be in a public location ➢ High risk of misaddressing the fax as it is reliant on a correct fax number being used	✓	✗	✗

UNIVERSITY OF LEICESTER

Data Protection (GDPR) Guidance Note No. 21

Organisational security measures:

Consider pseudonymisation of the data – this would involve sending the data using identifiers (i.e. student number) rather than a name and thereby minimising the risk if data loss occurs (do not send the pseudonymisation key via the same method).

Minimise what data is being sent – for example rather than sending the full information on a member of staff (DOB, medical history, marital status etc) only send those data fields that are relevant for the particular purpose.

Where possible avoid downloading data from source systems – report directly from the source system itself.

Do not send the password to an encrypted file via the same transfer method as the data transfer (it is recommended to verbally inform the recipient of the password).

Inform the recipient about the transfer and ask them to confirm that the data has been safely received.

When considering the transfer method consider both the data volume and the associated risk (i.e. it may be considered acceptable to email the data on 5 individuals, however this is highly likely not be the case if it is the data on 5000 individuals).

Use 7-Zip to encrypt files involving personal data regardless of the transfer method (see below for instructions).

Basic checks before transferring data:

1. Consider the nature of the data and the transfer method you are considering to determine what is appropriate.
2. Make sure you are sending the data to the correct individual. In general, you should avoid sending personal data to a group email.
3. Ensure you are sending the data to the correct recipient with the correct address and contact details – if in doubt double check to ensure you have the most up-to-date contact details.

The importance of passwords/passphrases

Strong passwords

- Strong passwords involve multiple upper and lower case characters, numbers and special characters
- They should be between 8 and 14 characters in length
- It's advisable not to use real words

Passphrases

- An even stronger approach is to use a passphrase.
- A passphrase is a sequence of words and is generally longer (and more secure) than a passowrd
- For example the phrase "My Favourite Book is the Famous Five by E. Blyton" could be turned into "Mf8!tF58yE8Lyt0n"

Communicating passwords

- Never send your passwords to a recipient via the same means as sending the data
- For example, if you sent the data via an encrypted email you should verbally inform the individual of the password.

UNIVERSITY OF LEICESTER

Data Protection (GDPR) Guidance Note No. 21

How to encrypt using 7-Zip:

1. Install 7-Zip via the Software Centre
2. Right click on the file to be zippd and from the menu select '7-Zip' and then 'Add to archive'
3. In the screen that appears, name the archive, choose encryption method AS256 (if not already selected) and set a password
4. The recipient will then need the password to decrypt it. Do not note the password in the Zip File

How to transfer using FileDrop:

1. In a browser on a managed PC/laptop, go to the following url: https://filedrop.le.ac.uk/
2. Login to the Filedrop service using you University IT account details (username and password)
3. Click the 'Drop-off' button and complete you name; organisation and email address (if these are not pre-completed), then click Next button
4. Make sure the options to send an email to the recipient and to notify sender when the file is collected are ticked
5. In the To: box, click the green '+' and type the recipient's email address
6. Click the 'Choose file' button and navigate to the file you want to send (preferably an encrypted .zip file)
7. Complete any file description or short note and click the 'Drop-off' button. Note: do not include the encrypted zip file's password!

Further information:

- If you need further information or have questions about transferring data email ithelp@leicester.ac.uk
- Further guidance on complying with the General Data Protection Regulations is available at: https://www.le.ac.uk/gdpr